



Universität Wien
Fakultät für Rechtswissenschaften

Wahlfachkorb Technologierecht
Ringvorlesung

Internet und Datenschutz
12. Oktober 2016

Ing. Mag. Dr. iur. Christof Tsohl



1



Der Referent / die Referentin

- ✓ Ing. Mag. Dr. iur. Christof Tsohl (36)
- ✓ Nachrichtentechniker (HTL, Ericsson, Kapsch) und Jurist
- ✓ Bis 2012 Ludwig Boltzmann Institut für Menschenrechte und Uni Wien
- ✓ Seit Ende 2012: Wissenschaftlicher Leiter und Gesellschafter der Research Institute AG & Co KG – Zentrum für digitale Menschenrechte und *Smart.Rights.Consulting*
- ✓ Forschung und Organisationsberatung – Schnittstelle von Technik und Recht
- ✓ Lehre (aktuell: Uni Wien, Lehrgang für Informations- und Medienrecht; Vienna Human Rights Master; Universität Hannover, Masterprogramme IT Law; Donau Uni Krems, Big Data und Datenschutz; FH St. Pölten: Ethik in der Technologieentwicklung; Anwaltsakademie Österreich)
- ✓ Mitgliedschaften:
 - Arbeitskreis Vorratsdaten Österreich (AKVorrat), Obmann
 - Österreichische Computer Gesellschaft (OCG), Arbeitskreisleiter „Forum Privacy“
 - Österreichische RichterInnenvereinigung, Fachgruppe Grundrechte, a.o. Mitglied, regelmäßig Vortragender in Aus- und Fortbildung seit 2008
 - Open Government Data Austria (OGD), Mitglied des wissenschaftlichen Beirats
 - Amnesty International, Mitglied



2



Grundlagen

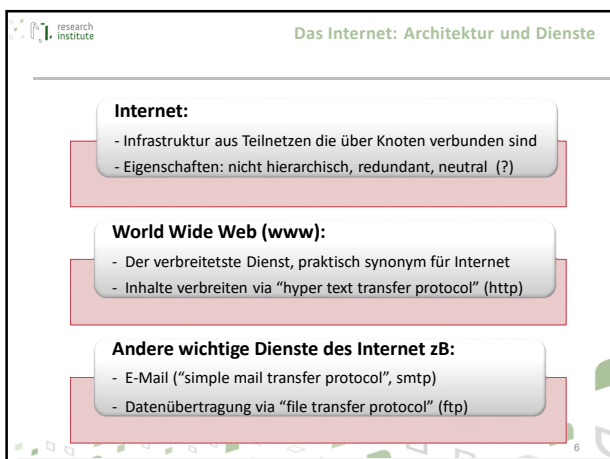
**Struktur des Internets und jüngere
technische und gesellschaftliche
Entwicklungen**

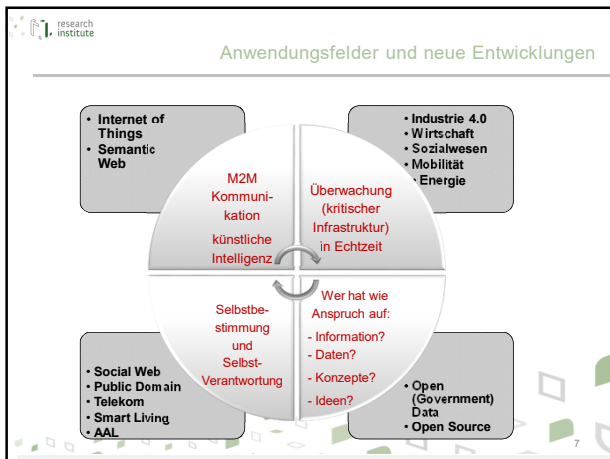


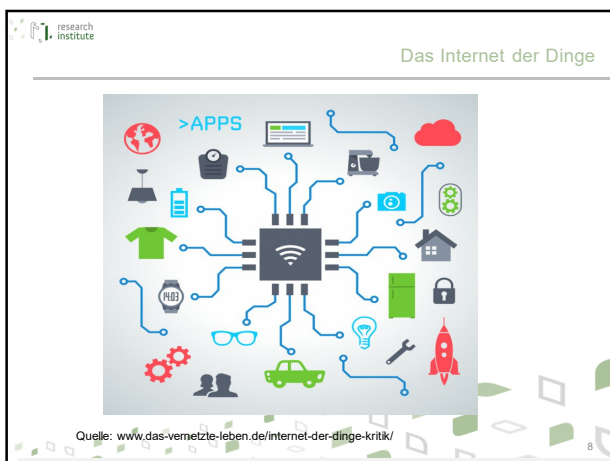
3

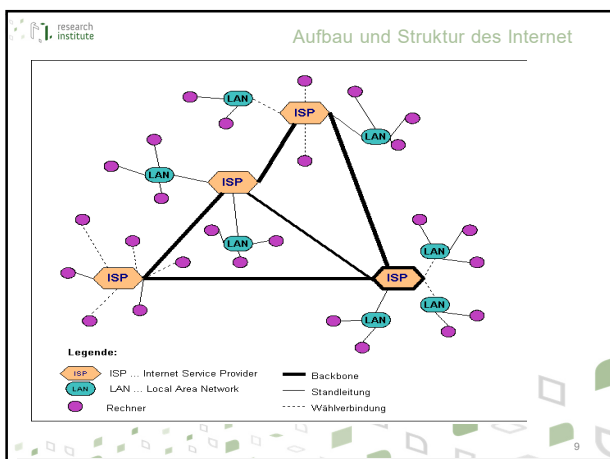


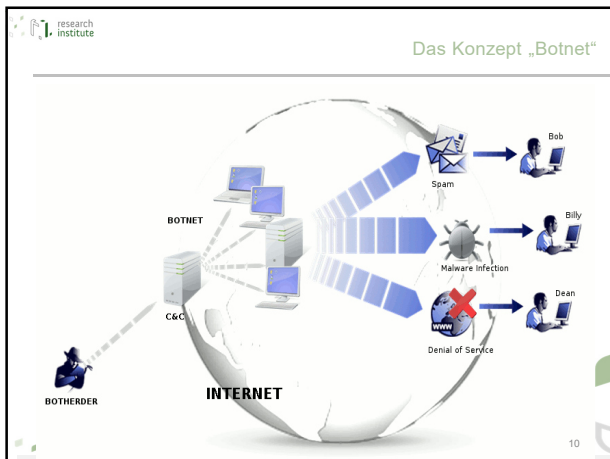


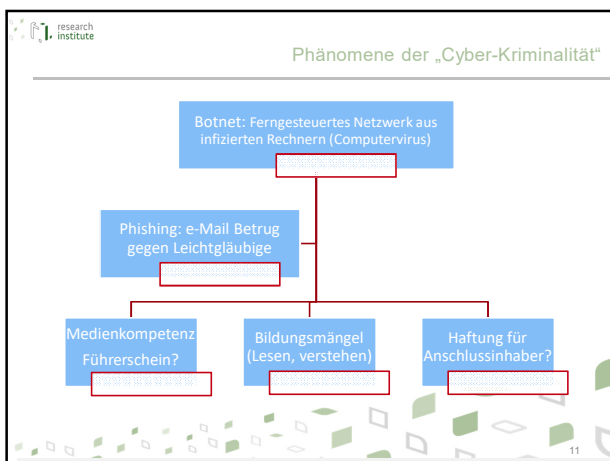


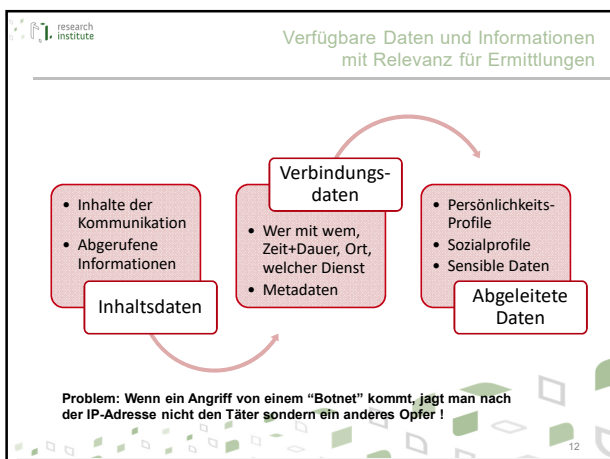


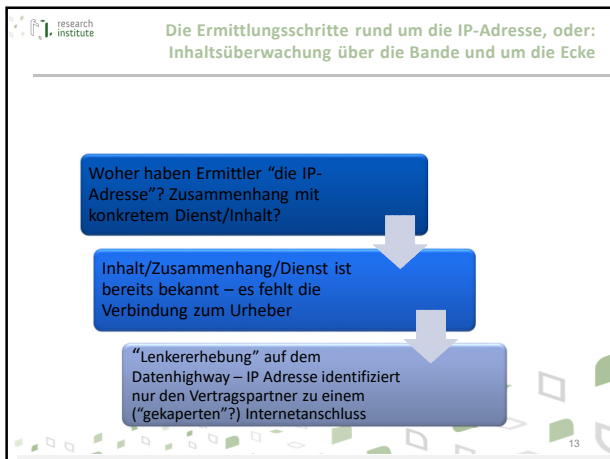


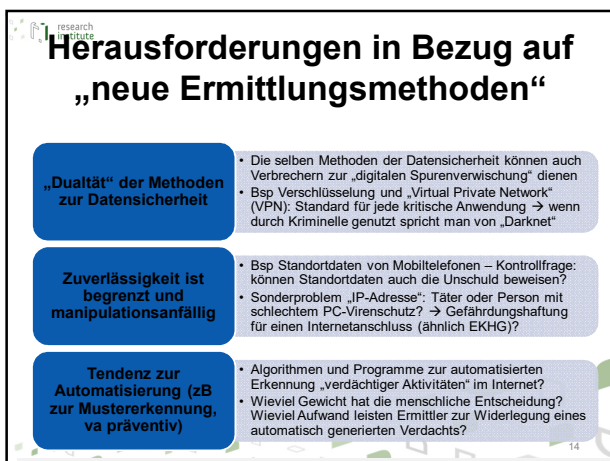


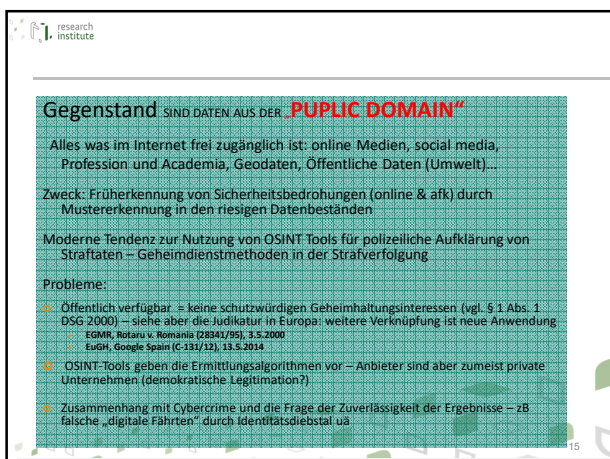












research institute

Datenschutz als Grundrecht / Menschenrecht



16

research institute

Moderne Grundrechte mit ausdrücklichem Bezug zur „digitalen Welt“

- ✓ **Grundrecht auf Datenschutz**
 - Ausdrücklich in Artikel 8 Grundrechte-Charta der EU garantiert
 - Recht auf Privat- und Familienleben parallel in Artikel 7 Grundrechte-Charta
 - Artikel 1: § 1 Datenschutzgesetz 2000 im Verfassungsrang (Datenschutzgrundrecht)
 - Verfassungsgerichtshof im „Vorratsdaten“-Urteil: „Recht auf informationelle Selbstbestimmung“
- ✓ **Deutschland:**
 - **Grundrecht auf „Informationelle Selbstbestimmung“**
 - **Grundrecht auf Vertraulichkeit und Integrität von Computersystemen**
 - Bundesverfassungsgericht schafft ein neues „Grundrecht auf Vertraulichkeit und Integrität von Computersystemen“, (kurz „Computer-Grundrecht“ – Entscheidung zum „Bundestrojaner“)
 - **Datenschutz ist nicht Selbstzweck – eher ein „Katalysator“**
 - zum Grundrechtsschutz in allen Bereichen
- ✓ **UN Menschenrechtsrat hat per Resolution A/HRC/20/L.13 klargestellt, dass alle Menschenrechte auch Online gelten → neuer Sonderberichterstatter eingerichtet!**

17

research institute

Selbstbestimmung und Eigenverantwortung in der digitalen Welt

Deutschland: Recht auf informationelle Selbstbestimmung (Art 1+2 GG)
Österreich: Grundrecht auf Datenschutz (§ 1 DSGVO)

Praktische Herausforderungen

Was einmal im Netz zugänglich ist, kann theoretisch endlos dupliziert werden	Kontrolle des Individuums über Datenverwendung in sozialen Netzwerken?
--	--

Eigenverantwortliches Management der „digitalen Identität“ (Profil)

Informierte Zustimmung und Verletzung der Zweckbindung: Aus der Initiative „Europe vs Facebook“ von Max Schrems – vgl. „Safe Harbour“ Urteil des EuGH (Große Kammer), 6.10.2015 („Schrems vs Irish Data Protection Commissioner“) C-362/14

Vgl. auch die Diskussion um das „Recht auf Vergessenwerden“
 derzeit explizit nur Recht auf Richtigstellung und Löschung im Einzelfall
 Vgl. aber Urteil des EuGH (Große Kammer), 13.5.2014 „Google Spain“ C-131/12

18

research institute

Recht auf Richtigstellung und Löschung Recht auf "Vergessenwerden" II

✓ „**Recht auf Vergessenwerden**“: Urteil des **EuGH** (Große Kammer) vom 13. Mai 2014 in der Rechtssache C-131/12, **Google Spain** SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González

- Bemerkenswert: Google unterliegt der EU Jurisdiktion und dem Datenschutzrecht, auch wenn in der EU nur eine Vertriebsniederlassung liegt
- Trefferliste zur Personensuche ist eine neue Informationskategorie und lässt das "Schutzwürdige Geheimhaltungsinteresse" (vgl. § 1 DSGVO) "wieder aufleben"
- Bedeutung für Ausnahme "öffentlich verfügbarer Daten" aus dem Schutzbereich?

19

research institute

Vorratsdatenspeicherung, oder: das Wechselbad der Paradigmen

EU Richtlinie 2006/24/EG: Öffentliche elektronische Kommunikation

- **Verbindungsdaten**: wer, mit wem, wann, wie lang, wo, welcher Dienst
- **Internet-Zugang**: IP-Adresse zu einem bestimmten Zeitpunkt
- **Flächendeckend auf Vorrat**, ohne konkreten Verdacht oder anderen Grund

Grundrechtseingriff ist unverhältnismäßig und daher nicht gerechtfertigt

- Pauschale Speicherung ohne Anlass und ohne Ausnahme ist überschießend
- Betrifft Privatsphäre, Datenschutz und freie Meinungsäußerung
- Besonderes Problem: Berufsgeheimnisse können umgangen werden

Aufhebung durch den Gerichtshof der EU (EuGH) am 8.4.2014

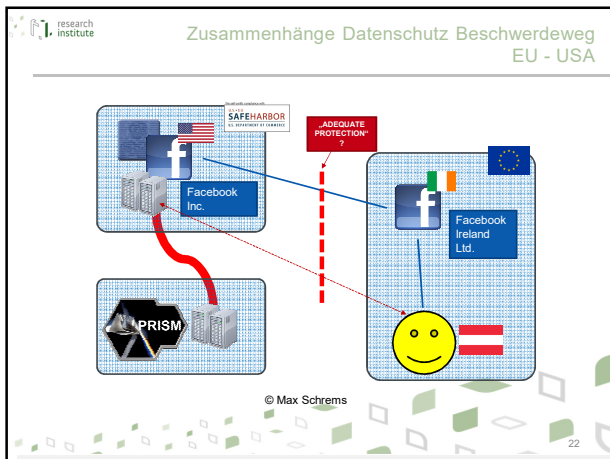
- Ua aufgrund österr. "Massenbeschwerde" an VfGH durch 11.139 Menschen
- Vorratsdatenspeicherung nach RL nicht vereinbar mit den EU Grundrechten
- Strafverfolgung zwar legitimes Ziel, Maßnahme aber überschießend
- Allfällige neue Richtlinie wird das Grundkonzept ändern müssen

20

research institute

Marktmacht und Rechtsdurchsetzung zB Initiative „Europe vs Facebook“ (Max Schrems)

21





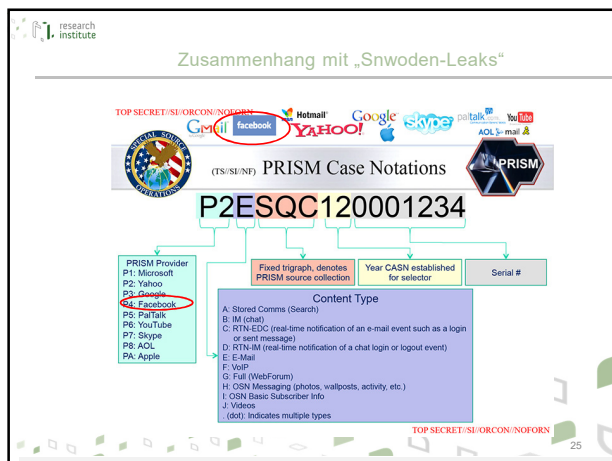
research institute

Vorabentscheidungsverfahren vor dem EuGH Gegenstand und Fragen

- ✓ **Entscheidung 2000/520 der Kommission auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46 (sog. „Safe Harbor Decision“)**
 - ✓ Angemessenes Schutzniveau besteht für einen US-amerikanischen Auftraggeber oder Dienstleister, wenn der für die Verarbeitung Verantwortliche die „Grundsätze des „sicheren Hafens“ zum Datenschutz (vorgelegt vom amerikanischen Handelsministerium am 21. Juli 2000) beachtet
 - ✓ „Selbst-Zertifizierung“ mit Bestätigung durch das US Handelsministerium
 - ✓ einseitige Anerkennung durch die EU Kommission (kein „Abkommen“ im rechtlichen Sinn)
- ✓ **Wesentliche Fragen:**
 - ✓ Hat die nationale Datenschutzbehörde Spielraum zur Prüfung im Einzelfall? (Rechtssicherheit?)
 - ✓ Ist die Entscheidung 2000/520 der Kommission „post-Snowden“ noch als mit der EU Grundrechte-Charta vereinbar zu sehen? (inzidente Normenkontrolle des EuGH)

research institute

24



Entscheidung des EuGH „Schrems C-362/14“ oder „Safe Harbor“-Urteil

- ✓ Rz 94: Insbesondere **verletzt** eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den **Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens**
- ✓ Rz 95: Desgleichen **verletzt** eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den **Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz**.

26

Konsequenzen der Safe Harbor Entscheidung des EuGH „Schrems C-362/14“

- ✓ Aufhebung der „Safe Harbor“ Entscheidung 2000/520 der Kommission
- ✓ Nationale Datenschutzbehörden dürfen durch auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46/EG ergangene Entscheidungen nicht beschränkt werden (Überschreitung der Zuständigkeit durch die Kommission)
- ✓ Nachfolgeregelung: „EU US Privacy Shield“

einige Verbesserungen

Problem im Kern unverändert

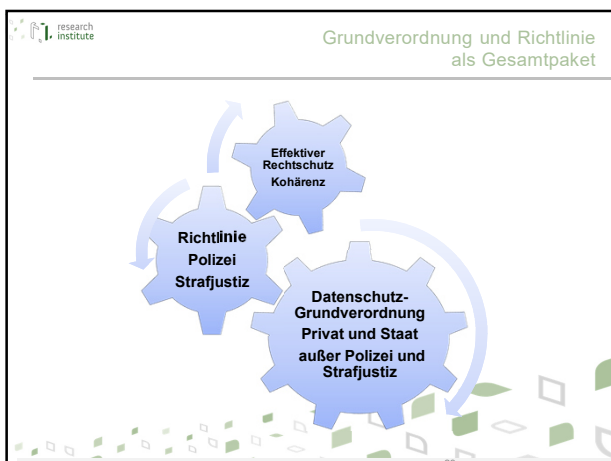
EU-US PRIVACY SHIELD

27

research institute

Neue Rechtsquellen auf EU-Ebene

- ✓ Datenschutz-Grundverordnung (DSGVO), VO 2016/679
 - Seit 24. Mai 2016 in Kraft; gilt ab 25. Mai 2018
 - Datenschutzrichtlinie (DSRL) tritt mit 25. Mai 2018 außer Kraft
 - Ziele und Grundsätze der DSRL gelten in der DSGVO fort
- ✓ Datenschutzrichtlinie für Polizei und Strafjustiz (DSRL-PJ), RL 2016/680
 - Erstmals einheitlicher Datenschutzrahmen für Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, Strafvollstreckung und Schutzes vor und Abwehr von Gefahren für die öffentliche Sicherheit (auch rein innerstaatliche Datenverarbeitung)
 - Seit 5. Mai 2016 in Kraft; von den Mitgliedstaaten bis 6. Mai 2018 umzusetzen
 - Rahmenbeschluss 2008/977/JI tritt mit 6. Mai 2018 außer Kraft



research institute

Datenschutz-Grundverordnung: Überblick

Verschärfung der Sanktionsmechanismen • Zivilrechtliche Haftung: Höchstbetrag auf 20 Millionen EUR oder 4 Prozent des weltweiten Jahresumsatzes des betroffenen Unternehmens (jeweils die höhere Summe) • Auch immaterielle Schäden • Verbandsklagen zulässig	Erhöhte Anforderungen an Datensicherheit • Datenschutz-Policy und geeignete technische und organisatorische Maßnahmen, alle 2 Jahre zu überarbeiten • Verpflichtende Risikoanalysen • Datenschutz-Folgenabschätzung • kontinuierliches "Lifecycle Datenschutz-Management"
Materiell-rechtliche Änderungen • zB IP-Adressen als personenbezogene Daten • zB Allgemeine "Data Breach Notification" • zB Recht auf „Vergessenwerden“	Verstärkte Kooperation der nationalen Datenschutzbehörden • „One-Stop-Shop“ Prinzip für Betroffene • neues Gremium "European Data Protection Board" (vgl. Art. 29 Gruppe, Europol JSB) • Mehr Koordination und Kohärenz

Datenschutz-Grundverordnung (DSGVO)

research institute

Grundrechte als Determinanten der Technologieentwicklung

„Human Dignity by Design“



31

research institute

Rahmenbedingungen der „Smart City“

The Need of Smart Rights for Smart Citizens

1. Technologie dient den Menschen und der Gesellschaft
2. Konzept hat Auswirkungen auf das soziale Gefüge
3. Komplexität erfordert Werte und Orientierungsnormen

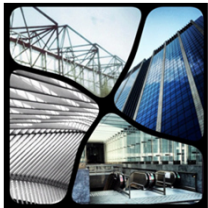
WERTE-RASTER oder die Suche nach dem kleinsten gemeinsamen Nenner in der Globalisierung

NORMATIVER RAHMEN birgt Dilemma zwischen Rechtssicherheit und notwendiger Dynamik

DATENSCHUTZ ist kein Selbstzweck → Katalysator für Grundrechte in der digital geprägten Welt

INFORMATIONSFREIHEIT UND TRANSPARENZ
Open Government Data / „wisdom of the crowd“

KRITISCHE INFRASTRUKTUREN sind exponiert (IT-)Sicherheit im Spannungsverhältnis zu Freiheit



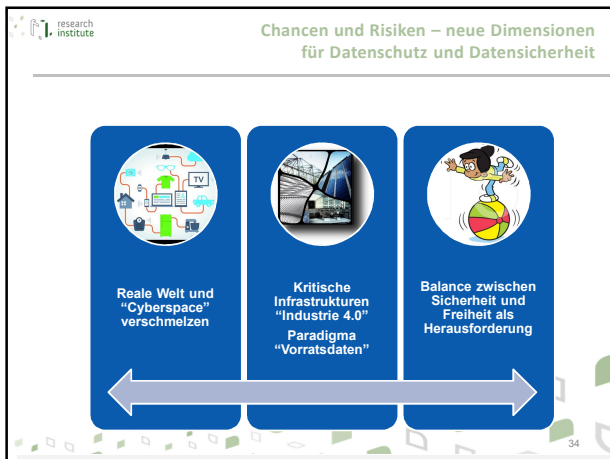
32

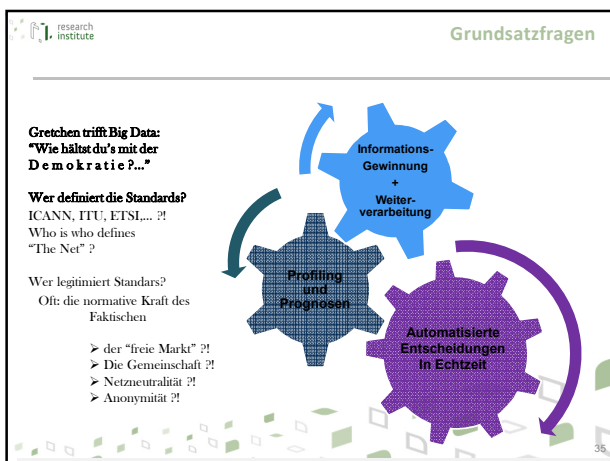
research institute

künstliche Intelligenz als „Entscheidungsträger“?



33









Der „Human Rights Based Approach“ als Maxime der Technologie-Entwicklung



Menschenrechte: gemeinsame internationale Determinanten für neue Technologien – Konkretisiert durch Rechtsprechung



Menschenrechtskonvention als „lebendiges Instrument“ (vgl. EGMR, Tyrer vs UK 1978)
UN Menschenrechtsrat: Resolution 2012 A/HRC/20/L.13 → **alle MR gelten auch „online“**



Unteilbarkeit der Menschenrechte: Immer das große Ganze sehen – **Balance und Grundsatz der Verhältnismäßigkeit**

37/37

research
institute

Notwendige Schritte
auf dem Weg zur menschenwürdigen „Smart City“

 Entwicklung der Konzepte und des Marktes Definition Rechtsrahmen und ethische Grundsätze	 soziale Verantwortung (CSR) durch die gesamte Wertschöpfungskette Staatliche Schutz- und Gewährleistungspflichten	 Stärkung der Eigenverantwortung der Menschen durch Bildung und Kompetenz im Umgang mit Technologie
--	---	---

36 36

research
institute

Abschluss / Ausblick

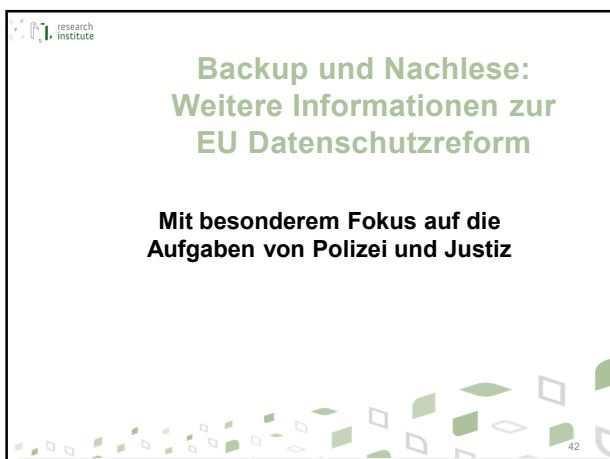
- ✓ Interdisziplinärer Austausch
Technologie/Gesellschaft/Recht
- ✓ Wirkungsfolgenabschätzung
Risikoabschätzung
- ✓ Klarer normativer Rahmen
transparente Vertragsgestaltung
- ✓ Stärkere Verantwortlichkeit von
Unternehmen
- ✓ Thinking by Design
Human Dignity by Design

Zeitalter der „Aufklärung 2.0“ und der Ausweg aus der
(selbstverschuldeten?) Unmündigkeit: wir sind NICHT machtlos!

39







research institute

Wichtige Neuerung der DSGVO im Überblick

Artikel 32 ff: Erhöhte Anforderungen an die Datensicherheit

- Schutz der Daten vor unbeabsichtigter oder widerrechtlicher Zerstörung, vor unbeabsichtigtem Verlust sowie zur Vermeidung jedweder unrechtmäßigen Verarbeitung, insbesondere jeder unbefugten Offenlegung, Verbreitung beziehungsweise Einsichtnahme oder Veränderung
- Weitere Konkretisierungen sowie Ermächtigung für „delegierte Rechtsakte“ vorgesehen
- Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
- Meldepflichten an Behörden und Informationspflichten an Betroffene („Data Breach Notification“)

Artikel 35: Verpflichtende Datenschutz-Folgenabschätzung

- Bei besonders risikobehafteten Datenanwendungen
- Demonstrative Aufzählung, insbesondere: **systematische und umfassende Bewertung persönlicher Aspekte** natürlicher Personen, beispielsweise zwecks **Analyse ihrer wirtschaftlichen Lage, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens** oder zwecks diesbezüglicher Voraussagen, die sich auf eine automatisierte Verarbeitung von Daten gründet

Artikel 42: programmatische Bestimmung zu Datenschutz-Zertifizierung

- Mitgliedstaaten und Kommission fördern insbesondere auf EU Ebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln
- Ziel: Rasche und einfache Kenntnis des Datenschutzniveaus
- Zweck: ordnungsgemäßen Anwendung der Datenschutz-Grundverordnung

43

research institute

Datenschutz-Richtlinie für den Polizei- und Strafrechtssektor (RL 2016/680)

Anwendungsbereich Sowohl grenzüberschreitende als auch nationale Sachverhalte

- *Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr*
- Sachlicher Anwendungsbereich: automatisierte oder manuell-strukturierte Datenverarbeitung
- Ausgenommen:
 - Wenn nicht im Anwendungsbereich des Unionsrechts, etwa im Bereich der nationalen Sicherheit
 - Datenverarbeitung durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union
 - Für diesen Bereich soll weiterhin Verordnung (EG) Nr. 45/2001 gelten (umstritten)

Regelungsdichte Kohärenz - weniger Umsetzungsspielraum als Rahmenbeschluss

- Erwägungsgründe zum Harmonisierungsbedarf und zur Subsidiarität:
- reibungsloser Transfer personenbezogener Daten innerhalb der EU
- EU weit wirksamer und Datenschutz Betroffener erfordert mehr Kohärenz
- **Ergänzung Parlament zu Art. 1: Strengere Vorschriften auf nationaler Ebene sollen zulässig sein**

44

research institute

Wichtige Neuerungen durch die Richtlinie im Überblick

Artikel 9: Profiling und automatischer Datenverarbeitung

- Ausschließlich automatisierte Datenverarbeitung mit nachteiligen Rechtsfolgen oder erheblicher Beeinträchtigung Betroffener zum Zwecke der Bewertung einzelner Aspekte ihrer Person sind grundsätzlich verboten → vgl. Art 15 Richtlinie 95/46/EG (Datenschutzrichtlinie)
- Ausnahmen müssen ausdrücklich gesetzlich vorgesehen sein und Schutzgarantien enthalten
- **Keinesfalls aber hinsichtlich „besonderer Kategorien personenbezogener Daten“ (Art 8)**
– vgl. „sensible Daten“ nach § 4 DSG

Artikel 11 – 16: Ausführlichere Regelung der Betroffenenrechte

- Rechte auf Information, Auskunft und deren Ausnahmen
- Rechte auf Berichtigung und Löschung (nicht neu) →
- strafrechtliche Ermittlungen und Strafverfahren: Verweis nationales Strafprozessrecht

Artikel 19: Datenschutz durch Technik und durch Voreinstellungen

- „Privacy by Design“ – „Privacy by Default“
- Art. 14: Protokollierung von Erhebung, Veränderung, Abfrage, Weitergabe, Kombination oder Löschung - Zweck, Datum und Uhrzeit der Vorgänge und möglichst Identität des Verarbeiters
- **Artikel 27 – Datensicherheit: Detaillierte Vorschriften, verpflichtende Risikoanalyse**
- **Artikel 28 – Verständigungspflichten an Aufsichtsbehörde bei Datenschutzverletzungen**

45

 research institute

Datenschutzgrundsätze (1/2)

- ✓ **Verhältnismäßigkeitsgrundsatz:** Kommt aus dem Datenschutz-Grundrecht (Art 8 Grundrechte-Charta bzw. Art 8 EMRK) und bezeichnet ein übergeordnetes Prinzip. Unter der „Verhältnismäßigkeit im engeren Sinn“ versteht man die Abwägung der Interessen bzw. Güter
- ✓ **Verbotsprinzip:** Die Verwendung personenbezogener Daten ist verboten, sofern sie nicht ausdrücklich erlaubt ist.
- ✓ **Zweckbindungsgrundsatz:** Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden.
- ✓ **Wesentlichkeitsgrundsatz:** Daten dürfen nur verwendet werden, soweit sie den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen.
- ✓ **Grundsatz der Datenlöschung:** Daten dürfen nur so lange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist.
- ✓ **Grundsatz der Datenminimierung:** Reduktion der Verarbeitung personenbezogener Daten auf das Unvermeidbare

46

 research institute

Datenschutzgrundsätze (2/2)

- ✓ **Privacy by Design und Privacy by Default**
- ✓ **Grundsatz von Treu und Glauben und Rechtmäßigkeit**
- ✓ **Grundsatz der Transparenz:** Information des Betroffenen über Vorhandensein einer Verarbeitung und deren Umstände
- ✓ **Grundsatz des Mitspracherechts:** Rechte auf Auskunft, Richtigstellung und Löschung sowie Widerspruch
- ✓ **Grundsatz der sachlichen Richtigkeit und Aktualität:** Daten dürfen nur so verwendet werden, dass sie im Hinblick auf den Verwendungszweck sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind.
- ✓ **Grundsatz der Datensicherheit**
- ✓ **Grundsatz der Rechenschaftspflicht**

47
